

 Georgia Technology Authority	<b>Georgia Technology Authority</b>	
<b>Title:</b>	<b>Security Log Management</b>	
<b>PSG Number:</b>	PS-08-022	
<b>Issue Date:</b>	3/20/2008	<b>Effective Date: 3/20/2008</b>
<b>Synopsis:</b>	Requires agencies to implement log management practices	

## PURPOSE

Developing, implementing and maintaining effective log management practices throughout an enterprise helps ensure that computer security events (actions of users, malicious activity and operational trends) are recorded and stored in sufficient detail and for an appropriate period of time as required by agency, state or federal regulation. Additionally, agencies with federal partners are subject to laws and regulations such as FISMA, GLBA, PCI and HIPAA that require or strongly recommend storage and review of certain logs. This policy establishes the requirement to implement log management practices for State information systems.

## SCOPE and AUTHORITY

- The authority to establish technology policies and standards is in O.C.G.A. 50-25-4(a)(10) and is explained in GTA policy “Information Technology Policies, Standards and Guidelines” PM-04-001.
- The authority to establish security policies and standards is in O.C.G.A. 50-25-4(a)(21) and is explained in GTA policy “Enterprise Information Security Charter” PS-08-005.

## POLICY

Agencies that operate and control State of Georgia information systems shall establish internal policies and procedures for creation, protection and retention of computer security logs and implement a log management infrastructure.

## RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Log Management Infrastructure (SS-08-036)

## REFERENCES

NIST 800-92 Guide to Computer Security Log Management

## TERMS AND DEFINITIONS

**Log** - A record of the events occurring within an organization’s systems and networks.

**Computer Security Log Management** - The processes for generating, transmitting, storing, analyzing and disposing of computer security log data.

**Log Management Infrastructure** - Consists of the hardware, software, networks and media used to generate, transmit, store, analyze, and dispose of log data.